107TH CONGRESS
2D SESSION

S. 2629

To provide for an agency assessment, independent review, and Inspector General report on privacy and data protection policies of Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 17, 2002

Mr. DASCHLE (for Mr. TORRICELLI) introduced the following bill; which was read twice and referred to the Committee on Governmental Affairs

---

A BILL

To provide for an agency assessment, independent review, and Inspector General report on privacy and data protection policies of Federal agencies, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. PRIVACY AND DATA PROTECTION POLICIES OF FEDERAL AGENCIES.

(a) SHORT TITLE.—This Act may be cited as the ''Federal Privacy and Data Protection Policy Act of 2002''.

(b) DEFINITIONS.—In this Act, the term ''agency'' has the meaning given that term under section 551(1) of title 5, United States Code.

(c) FINDINGS.—Congress finds that—

(1) in the wake of the attacks on the United States on September 11, 2001, Federal agencies are collecting an increasing amount of personal information from and on individuals as part of the expanded war on terrorism;

(2) the worthwhile goals of those data collection initiatives are to help ensure homeland security and protect the people of the United States from future acts of terrorism;

(3) protecting homeland security and fighting terrorism requires not only seeking to protect lives and property in the United States, but also ensuring that individual rights and essential liberties are safeguarded;

(4) in order to achieve these goals, it is essential that agencies properly manage, maintain, and secure personal information on people in the United States from inappropriate use, disclosure, or dissemination to third parties;

(5) because of the leading role of the Federal Government in the expanded war on terrorism, the

Federal Government should serve as a role model for State and local government, and the private sector, by establishing effective safeguards and procedures to protect personal data of people in the United States;

(6) in order to ensure that people in the United States understand and have confidence in the proper use and safety of personal information, it is essential for agencies to implement effective privacy policies and procedures and to state those privacy policies, both online and offline; and

(7) an essential part of ensuring that the people in the United States have full confidence in the privacy and security of personal information is to—

(A) have agencies confirm adherence by those agencies to the stated policies; and

(B) have independent, third party review, and confirmation of adherence.

(d) PURPOSE.—The purpose of this Act is to provide a framework for ensuring effective data and privacy management by Federal agencies to—

(1) ensure public confidence and trust in how agencies collect, maintain, and use personal information;

(2) ensure continued adherence to data protection and privacy policies and procedures;

(3) ensure that individual rights and essential liberties are protected; and

(4) provide for effective oversight of the collection and use of individual information.

(e) PRIVACY MANAGER.—

(1) IN GENERAL.—Each agency shall designate an employee of that agency as the agency privacy manager to—

(A) be responsible for effective data protection and management within that agency; and

(B) ensure compliance with the privacy and data security policies.

(2) ADDITIONAL RESPONSIBILITIES.—Each privacy manager shall be responsible for—

(A) training and education for employees to promote awareness of and compliance with the privacy and data security policies; and

(B) developing recommended practices and procedures to ensure compliance with the privacy and data security policies.

(f) BENCHMARK ASSESSMENT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, each agency shall

conduct a detailed benchmark assessment of the privacy and data protection policies and practices of that agency with regard to the collection, use, sharing, disclosure, transfer, and security of personally identifiable information relating to the agency employees and the public. Such practices shall be accurately and clearly stated in written policies governing the data collection and use practices of the agency, both online and offline.

(2) CONTENT.—At a minimum, each benchmark assessment shall determine and state—

(A) the personally identifiable information the agency collects on—

(i) employees of the agency; and

(ii) members of the public;

(B) any purpose for which the personally identifiable information is collected;

(C) any notice given to individuals regarding the collection and use of personal information, relating to that individual;

(D) any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual;

(E) whether or not consent is obtained from an individual before personally identifiable

information is collected, used, transferred, or disclosed and any method used to obtain consent;

(F) the policies and practices of the agency for the security of personally identifiable information;

(G) the policies and practices of the agency for the proper use of personally identifiable information;

(H) the training and education procedures of the agency to adequately train personnel on agency policies and procedures for privacy and data protection;

(I) the policies and procedures of the agency for monitoring and reporting violations of privacy and data protection policies; and

(J) the policies and procedures of the agency for assessing the impact of technologies on the stated privacy and security policies.

(g) RECORDING.—A written report of each benchmark assessment shall be prepared and recorded with the Inspector General of the agency to serve as a benchmark for the data protection and privacy practices and policies of the agency. Each benchmark assessment shall be signed by the agency privacy manager, verifying that the agency

is in good faith compliance with the policies and practices stated in the benchmark assessment.

(h) INDEPENDENT, THIRD-PARTY REVIEW.—

(1) IN GENERAL.—At least every 3 years, each agency shall have performed an independent, third-party review of the privacy and data protection practices of the agency to—

(A) determine the effectiveness of the privacy and data protection policies, practices, and procedures; and

(B) ensure compliance with the stated privacy policy of the agency.

(2) PURPOSES.—The purposes of reviews under this subsection are to—

(A) measure privacy and data protection practices against the original benchmark assessment of the agency;

(B) ensure compliance and consistency with both online and offline stated privacy policies; and

(C) provide agencies with ongoing awareness and recommendations regarding privacy and data protection practices.

(3) REQUIREMENTS OF REVIEW.—The Inspector General of each agency shall contract with an

independent, third party that is a recognized leader in privacy consulting, privacy technology, and data collection and use management to—

(A) evaluate the privacy and data protection practices of the agency; and

(B) recommend strategies and specific steps to improve privacy and data protection management.

(4) CONTENT.—Each review under this subsection shall include—

(A) a review of the original benchmark assessment concerning the privacy and data protection practices of the agency with regard to the collection, use, sharing, disclosure, transfer, and security of personally identifiable information relating to agency employees and the public;

(B) a detailed review of the current offline privacy and data protection practices of the agency with regard to the collection, use, sharing, disclosure, transfer, and security of personally identifiable information of the employees of the agency and the public to check for compliance with the original benchmark assessment, especially concerning whether those practices

are accurately reflected in the written policies of the agency; and

(C) a detailed electronic scan of any website of the agency with a technology product that alerts an agency to the privacy vulnerabilities on that web page, including—

(i) possible noncompliance with the benchmark assessment;

(ii) whether the privacy and data protection practices of the agency comply to the written privacy policy of the agency; and

(iii) whether there are any risks for inadvertent release of personally identifiable information from the website of the agency.

(5) RESTRICTIONS TO AVOID CONFLICT OF INTEREST.—An independent contractor that has substantial business with an agency may not perform a review under this subsection for that agency.

(6) REPORT.—Upon completion of a review, the Inspector General of an agency shall submit to the head of that agency a detailed report on the review, including recommendations for improvements or en-

hancements to privacy and data protection practices of the agency.

(i) INTERNET AVAILABILITY.—Each agency shall make each agency benchmark assessment, each independent third party review, and each report of the Inspector General relating to that review available to the public on the website of the agency.

○